Journal scientific and applied research, vol. 5, 2014
Association Scientific and Applied Research
International Journal

Original Contribution

ISSN 1314-6289

VULNERABILITY PENETRATION TESTING THE COMPUTER AND NETWORK RESOURCES OF WINDOWS BASED OPERATING SYSTEMS

Petar Boyanov

KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN,
SHUMEN 9712, 115, UNIVERSITETSKA STR,
E-MAIL: peshoaikido@abv.bg

Abstract: *In this paper a vulnerability penetration testing for several hosts in WLAN is made. The exploited operating systems were Microsoft Windows 7Enterprise and Microsoft Windows 8. It has been used an exploit named "Java storeImageArray () Invalid Array Indexing Vulnerability". Thanks to the open source penetration testing platform - Metasploit Framework the exploit was executed on the target hosts. The most important and critical reason the attack being successfully executed is connected with the human factor and intervention. Thereby, some security professionals and network administrators can use Metasploit Framework neither to run exploit nor to write security scripts in order to detect and protect the computer and network resources against various malicious cyber-attacks.*

Key words: *Computer and network security, cyber-attacks, Penetration, Vulnerability, Windows 7, Windows 8.*

1. Introduction

Most of the cyber-users allow being installed different online applications into their computer and network systems. In addition to these applications some cyber-criminals and malicious users send special IPv4 addresses and internet hyperlinks to marked victims in order to gain an unauthorized access to their computer and network resources. Unfortunately most of the users have not the slightest notion that is the purpose of these sent IP addresses and internet hyperlinks and as result of this execution they shall become victims. Therefore the whole set of confidential information could be stolen and public exposured. In this paper penetration vulnerability in the operating systems - Microsoft Windows 7 (Build 7601) Enterprise SP1 and Microsoft Windows 8 (Build 9200) is found. The whole experiment in specialized computer laboratory is made [3],[5].

This paper is structured as follows. First, in section 2, a detail survey of the structure and functions for Metasploit Framework is made. After that, in section 3, the process of exploitation in the target hosts in the WLAN (1.1.1.0/24) is performed. The achieved results are presented in section 4. The final conclusions and recommendations are made in section 5.

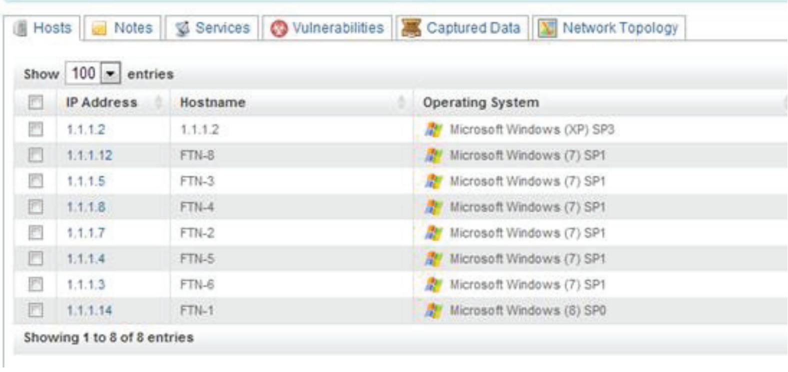
2. Related work

In [1] a specific methodology for penetration tester and penetration testing team is given. Common hacking tools for Linux and Windows based operating systems by Fox, Erin, Jeremiah Bush, Sylvia Ashley, and Ian Webb are analyzed tested and evaluated [2]. In [3] the details and functions of the Metasploit Framework by Carlos Joshua Marquez are explained and tested. In [4] a brief description of the whole structure of the Metasploit Framework and Metasploit Project by H. D. Moore is presented and explained. In [5] several free and open source tools as well as techniques to simulate malicious cyber-attacks by Nishant Shrestha are illustrated and made.

3. Experiment

The experiment in specialized Wireless Local Area Network (WLAN) is made. This network has consisted of 15 hosts and each of them has used a 150Mbps Wireless N USB Adapter TL-WN721N. In the computer laboratory a 150Mbps Wireless N Router TL-WR741ND has been used. The Dynamic Host Configuration Protocol (DHCP) in the router's configuration has been activated in order to each host to obtain a valid IPv4 address, network mask, default gateway and DNS server address. The network id of this WLAN is 1.1.1.0/24. The attacking host has used Microsoft Windows 7 Enterprise SP1 operating system and special software named Metasploit Framework. In actual fact Metasploit is an open source penetration testing and development platform. With this software each user is able to gain access to computer and network resources of the selected victim. In addition each user can write own exploit code [1],[3] in order to find new vulnerabilities [4].

The first step with the finding of active hosts was connected. On fig.1 the number of the active hosts is shown.



Show 100 entries

□	IP Address	Hostname	Operating System
□	1.1.1.2	1.1.1.2	Microsoft Windows (XP) SP3
□	1.1.1.12	FTN-8	Microsoft Windows (7) SP1
□	1.1.1.5	FTN-3	Microsoft Windows (7) SP1
□	1.1.1.8	FTN-4	Microsoft Windows (7) SP1
□	1.1.1.7	FTN-2	Microsoft Windows (7) SP1
□	1.1.1.4	FTN-5	Microsoft Windows (7) SP1
□	1.1.1.3	FTN-6	Microsoft Windows (7) SP1
□	1.1.1.14	FTN-1	Microsoft Windows (8) SP0

Showing 1 to 8 of 8 entries

Fig.1. The active hosts on network 1.1.1.0/24

Fig.1 has showed that 8 hosts are in an active state. Host on 1.1.1.2 has been running Microsoft Windows XP SP3, hosts on 1.1.1.12, 1.1.1.5, 1.1.1.8, 1.1.1.7, 1.1.1.4, 1.1.1.3 have been running Microsoft Windows 7 SP1 and host on 1.1.1.14 has been running Microsoft Windows 8 SP0.

The name of the used the exploit was "**Java storeImageArray () Invalid Array Indexing Vulnerability**". This exploit [2] in several security vulnerability databases was indexed. This exploit used vulnerability in the Java Runtime Environment (JRE) component in Oracle SE 7 Update 7, 11, 21, 25 and previous, 6 Update 45 and previous. This exploit caused critical damages to the selected computer and network system. The details of this vulnerability [5] were known as:

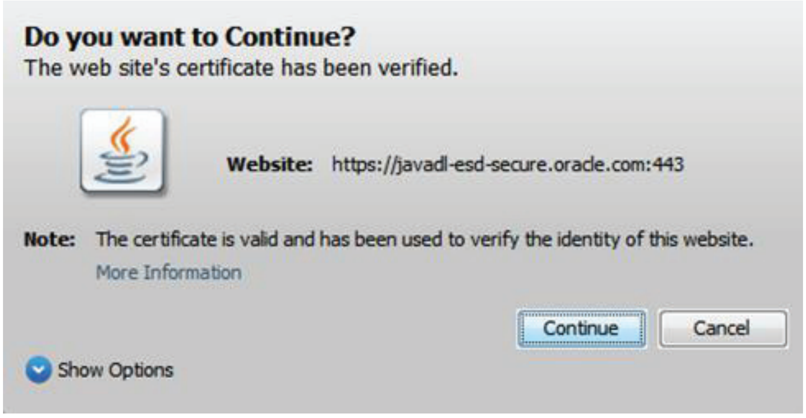
- CVE-2013-2465;
- OSVDB-96269;
- EDB-27526 and etc.

The next step with the configuration of this exploit in the Metasploit Framework was connected.

The following steps were made:

- SRVHOST was set on host with IP address 1.1.1.9 because this was the attacking host;
- SRVPORT was set on port 8080 because this exploit would be executed vie http protocol [4],[5];
- Listener Host was se again on host with IP address 1.1.1.9;
- URIPATH was set as follows: http://1.1.1.9:8080/university_project.html.

The aim of this URL was to be sent on the selected victim. After sending of the malicious hyperlink, the marked user had to allow the java web site's certificate. This is shown on fig.2.



Do you want to Continue?

The web site's certificate has been verified.

Website: https://javadl-esd-secure.oracle.com:443

Note: The certificate is valid and has been used to verify the identity of this website.

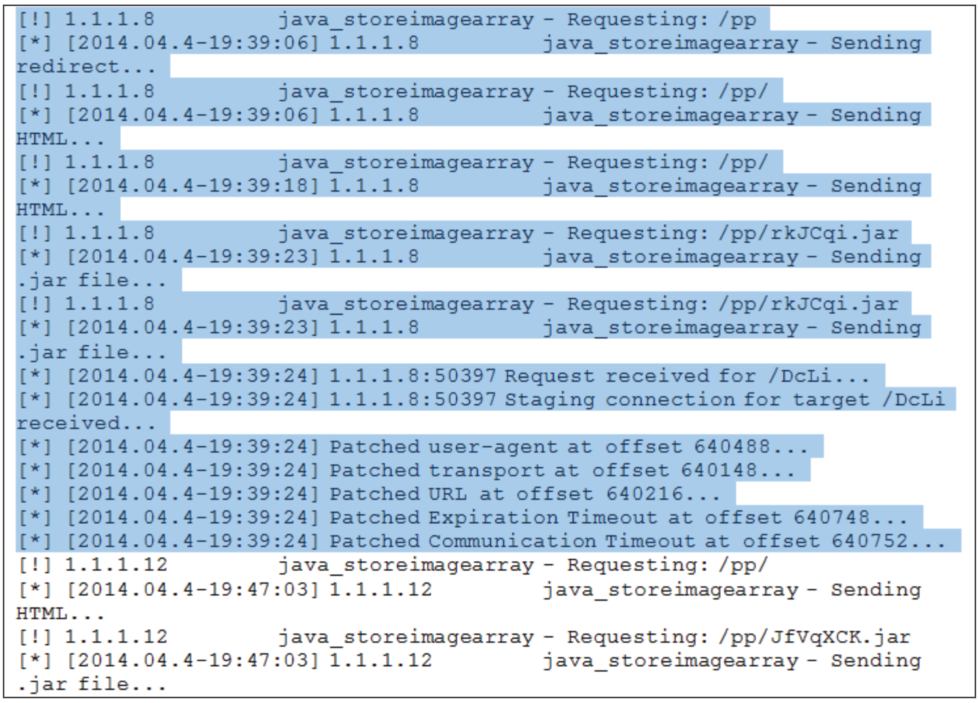
More Information

Fig.2. The verifying the identity of this website

After selecting the button “Continue”, the marked victim was successfully exploited using Metasploit Pro and thereby, the malicious user has obtained access to confidential data of the victim.

4. Results

Thanks to the generated PDF export, on fig.3 the whole vulnerability penetration progress on host with IP address 1.1.1.8 was shown.



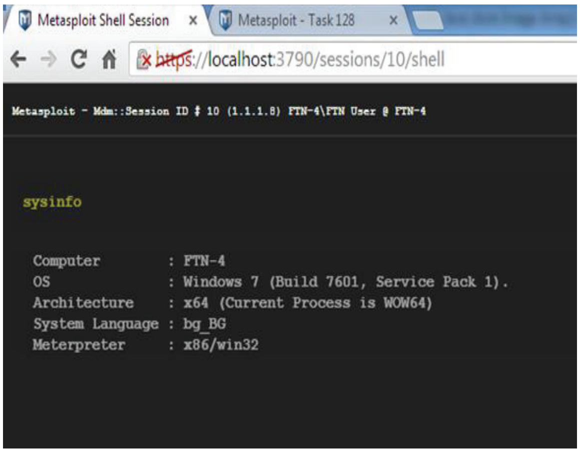
```
[!] 1.1.1.8          java_storeimagearray - Requesting: /pp
[*] [2014.04.4-19:39:06] 1.1.1.8          java_storeimagearray - Sending
redirect...
[!] 1.1.1.8          java_storeimagearray - Requesting: /pp/
[*] [2014.04.4-19:39:06] 1.1.1.8          java_storeimagearray - Sending
HTML...
[!] 1.1.1.8          java_storeimagearray - Requesting: /pp/
[*] [2014.04.4-19:39:18] 1.1.1.8          java_storeimagearray - Sending
HTML...
[!] 1.1.1.8          java_storeimagearray - Requesting: /pp/rkJCqi.jar
[*] [2014.04.4-19:39:23] 1.1.1.8          java_storeimagearray - Sending
.jar file...
[!] 1.1.1.8          java_storeimagearray - Requesting: /pp/rkJCqi.jar
[*] [2014.04.4-19:39:23] 1.1.1.8          java_storeimagearray - Sending
.jar file...
[*] [2014.04.4-19:39:24] 1.1.1.8:50397 Request received for /DcLi...
[*] [2014.04.4-19:39:24] 1.1.1.8:50397 Staging connection for target /DcLi
received...
[*] [2014.04.4-19:39:24] Patched user-agent at offset 640488...
[*] [2014.04.4-19:39:24] Patched transport at offset 640148...
[*] [2014.04.4-19:39:24] Patched URL at offset 640216...
[*] [2014.04.4-19:39:24] Patched Expiration Timeout at offset 640748...
[*] [2014.04.4-19:39:24] Patched Communication Timeout at offset 640752...
[!] 1.1.1.12         java_storeimagearray - Requesting: /pp/
[*] [2014.04.4-19:47:03] 1.1.1.12         java_storeimagearray - Sending
HTML...
[!] 1.1.1.12         java_storeimagearray - Requesting: /pp/JfVqXCK.jar
[*] [2014.04.4-19:47:03] 1.1.1.12         java_storeimagearray - Sending
.jar file...
```

Fig.3. The successful executed exploit on host with IP address 1.1.1.8 and that was running Microsoft Windows 7 (Build 7601) Enterprise SP1

The available actions on this host were:

- Collect System Data [3] - this allows being collected system evidence like screenshots, passwords, system information, etc.
- Virtual Desktop - this allows being viewed the current desktop on the victim machine.
- Access Filesystem - this allows being downloaded, uploaded and even deleted files from the target host.
- Search Filesystem - this allows being searched determined files.
- Command Shell - this allows being used the remote command shell terminal on the victim. It is recommended to be used by advanced users.
- Create Proxy Pivot - this allows being executed proxy server attacks on the victim.
- Create VPN Pivot - this allows being executed VPN Server attacks on the victim.

- Terminate Session - this allows being closed the current session with the compromised host.
- Session History, etc. On fig.4. the command shell terminal on the target host is shown.

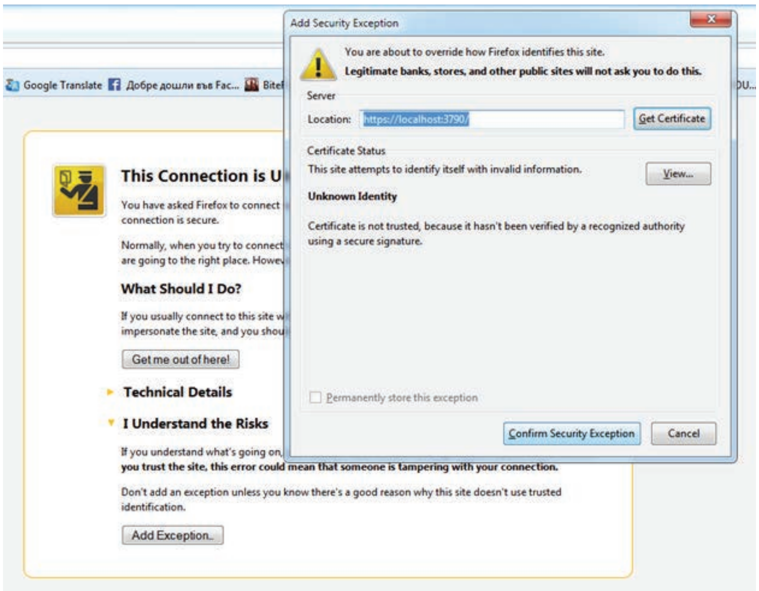


```
Metasploit - Mdm::Session ID # 10 (1.1.1.8) FTN-4\FTN User @ FTN-4


 sysinfo

  Computer        : FTN-4
  OS              : Windows 7 (Build 7601, Service Pack 1).
  Architecture    : x64 (Current Process is WOW64)
  System Language : bg_BG
  Meterpreter     : x86/win32
```

Fig.4. The executed command “sysinfo” on the target machine

From fig.4 there could be seen that the computer name was “FTN-4”, operating system was “Windows 7 (Build 7601, Service Pack 1), architecture was “x64 (Current Process is WOW64), system language was “bg_BG” and payload type (Meterpreter) is “x86/win32”.

On host with IP address 1.1.1.14 this exploit was also successfully executed. The operating system that was running on this host was Microsoft Windows 8 (Build 9200). The verifying the identity of this website is shown on fig.5.



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Location: https://localhost:3790/

This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

□ Permanently store this exception

This Connection is U

You have asked Firefox to connect connection is secure.

Normally, when you try to connect are going to the right place. Howe

What Should I Do?

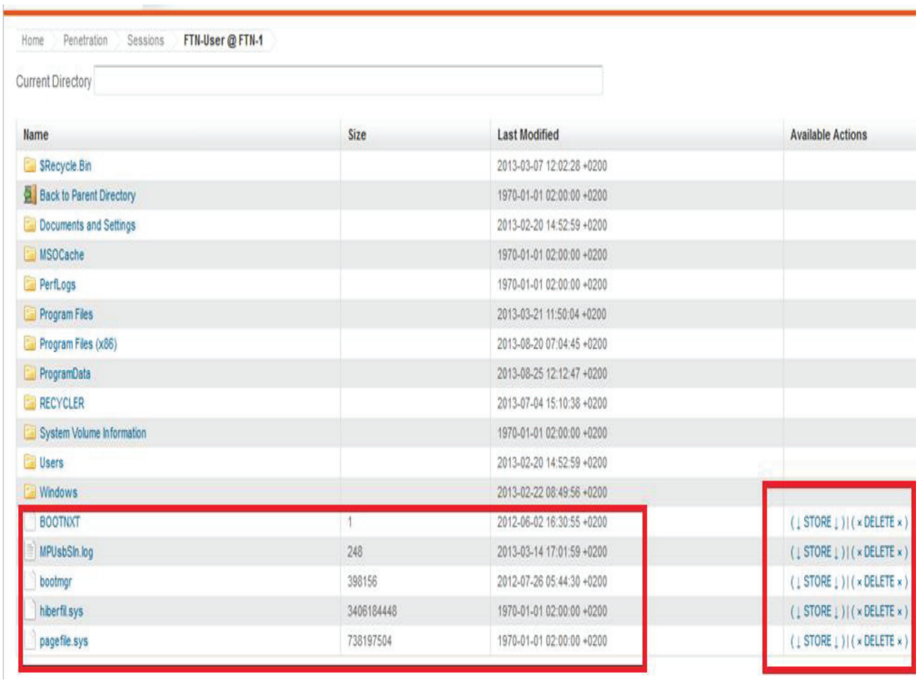
If you usually connect to this site w impersonate the site, and you shou

If you understand what's going on, **you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Fig.5. Adding Security Exception to the selected website

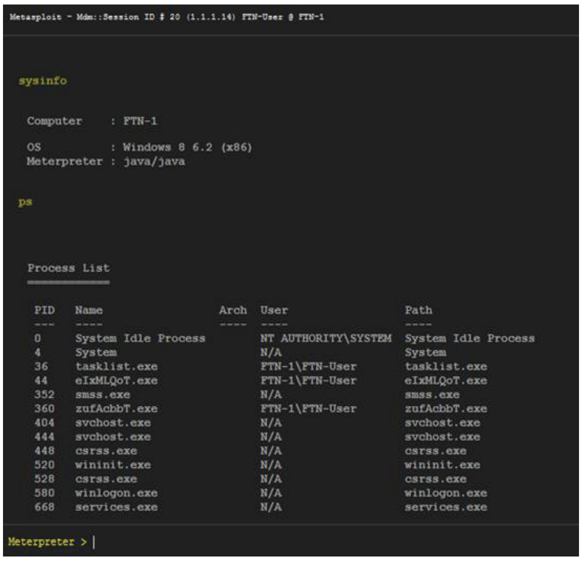
Most of the plain users should understand that this task is forbidden to be done. Otherwise the user accept to be shelled and public exposured. The sentence with the bold font must be remembered - “Legitimate banks, stores and other public sites will not ask you to do this.”



Name	Size	Last Modified	Available Actions
$Recycle.Bin		2013-03-07 12:02:28 +0200	
Back to Parent Directory		1970-01-01 02:00:00 +0200	
Documents and Settings		2013-02-20 14:52:59 +0200	
MSOCache		1970-01-01 02:00:00 +0200	
PerfLogs		1970-01-01 02:00:00 +0200	
Program Files		2013-03-21 11:50:04 +0200	
Program Files (x86)		2013-08-20 07:04:45 +0200	
ProgramData		2013-08-25 12:12:47 +0200	
RECYCLER		2013-07-04 15:10:38 +0200	
System Volume Information		1970-01-01 02:00:00 +0200	
Users		2013-02-20 14:52:59 +0200	
Windows		2013-02-22 08:49:56 +0200	
BOOTNXT	1	2012-06-02 16:30:55 +0200	(↓ STORE ↓) | (× DELETE ×)
MPUsbSIn.log	248	2013-03-14 17:01:59 +0200	(↓ STORE ↓) | (× DELETE ×)
bootmgr	398156	2012-07-26 05:44:30 +0200	(↓ STORE ↓) | (× DELETE ×)
hiberfil.sys	3406184448	1970-01-01 02:00:00 +0200	(↓ STORE ↓) | (× DELETE ×)
pagefile.sys	738197504	1970-01-01 02:00:00 +0200	(↓ STORE ↓) | (× DELETE ×)

Fig.6. Access to the filesystem on host with IP address 1.1.1.14 that was running Microsoft Windows 8 (Build 9200)

Fig.6. showed that the malicious user was able to delete very critical systems files like bootmgr, hiberfil.sys, pagefile.sys, BOOTNXT, etc. After deleting these files on the next reboot of this machine the current operating system would not be started and this would cause serious problems to the plane user. It is important to be understood that the malicious user could be able to install a hidden agent application with that to establish remote connection with the victim every time when the target is online in Internet public space.



```
Metasploit - Mdm::Session ID # 20 (1.1.1.14) FTN-User @ FTN-1

sysinfo

 Computer    : FTN-1

 OS          : Windows 8 6.2 (x86)
 Meterpreter : java/java

ps

 Process List
 ============

  PID   Name                 Arch  User                    Path
  ---   ----                 ----  ----                    ----
  0     System Idle Process        NT AUTHORITY\SYSTEM     System Idle Process
  4     System                     N/A                     System
  36    tasklist.exe               FTN-1\FTN-User          tasklist.exe
  44    eIxMLQoT.exe               FTN-1\FTN-User          eIxMLQoT.exe
  352   smss.exe                   N/A                     smss.exe
  360   zufAcbbT.exe               FTN-1\FTN-User          zufAcbbT.exe
  404   svchost.exe                N/A                     svchost.exe
  444   svchost.exe                N/A                     svchost.exe
  448   csrss.exe                  N/A                     csrss.exe
  520   wininit.exe                N/A                     wininit.exe
  528   csrss.exe                  N/A                     csrss.exe
  580   winlogon.exe               N/A                     winlogon.exe
  668   services.exe               N/A                     services.exe

Meterpreter > |
```

Fig.7. The executed commands “sysinfo” and “ps” on the target machine

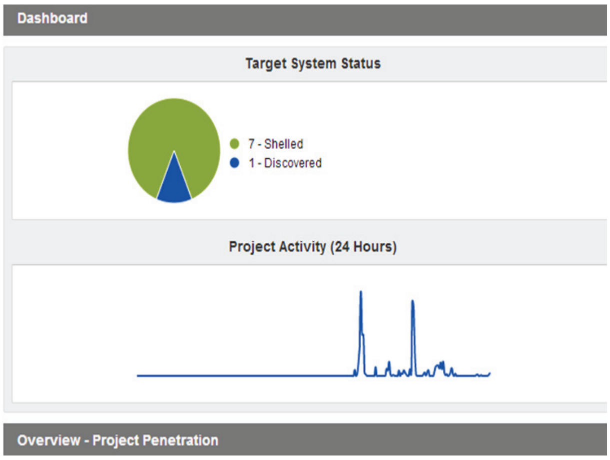


Fig.8. The status of the hosts and the project activity

5. Conclusion

In this paper a specialized vulnerability penetration testing of several target hosts is made. Thanks to the achieved results each host was compromised and shelled. The exploit “Java storeImageArray () Invalid Array Indexing Vulnerability” was successfully executed on the target machines. With the following sent hyperlink via http - http://1.1.1.9:8080/university_project.html, almost of all target hosts have accepted this security risk. Regardless of the operating system (Windows 7 or Windows 8) the exploit was successfully executed thanks to the vulnerability in Java Runtime Environment. Therefore, it is strongly recommended each user to update the java software with the latest stable version. The java versions that are vulnerable to exploitation are 7 Update 7, 11, 21, 25 and previous, 6 Update 45 and previous versions. At the moment the best stable version of java is version 7 update 51. Another important feature is connected with the Java Control Panel and it is also recommended the security level to be set to “very high” in order the plane users to protect their computer and network resources from future various malicious cyber-attacks.

Acknowledgements

This paper is supported by the Project BG051PO00l-3.3.06-0003 “Building and steady development of PhD students, post-PhD and young scientists in the areas of the natural, technical and mathematical sciences”. The Project is realized by the financial support of the Operative Program “Development of the human resources” of the European social found of the European Union.

References:

[1] Bhattacharyya, Debnath, and Farkhod Alisherov. "Penetration testing for hire." International Journal of Advanced Science and Technology 8 (2009).

[2] Fox, Erin, Jeremiah Bush, Sylvia Ashley, and Ian Webb. "Common Hacking Tools for Linux and Windows." (2002).

[3] Marquez, J. "An Analysis of the IDS Penetration Tool: Metasploit." The InfoSec Writers Text Library, Dec 9 (2010).

[4] Moore, H. D. "Metasploitation." In CanSecWest Security Conference 2008. 2006.

[5] Shrestha, Nishant. "Security Assessment via Penetration Testing: Network and System Administrator's Approach: Security, Network and System Administrator, Penetration Testing." (2012).